BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era sekarang banyak individu maupun organisasi yang mulai bergantung pada komputer dan internet sebagai media untuk bekerja maupun bersosial, dikarenakan komputer dan internet dapat mempermudah pengiriman data secara jarak jauh. Namun dengan adanya komputer dan internet tidak menutup kemungkinan bahwa pencurian data tidak bisa dilakukan. Maka dari itu sekarang keamanan siber sangat diperhatikan oleh beberapa individu maupun organisasi. Beberapa contoh penyerangan siber seperti *phising,malware,credential reuse,man in the middle*, dan lain-lain dapat merugikan suatu individu maupun kelompok dalam bentuk kehilangan dokumen penting atau data-data pribadi yang tersebar luas. Dan ada juga serangan siber yang dinamai rekayasa sosial, dimana rekayasa sosial merupakan serangan siber yang berbahaya dan melakukan penyerangannya melalui beberapa aspek seperti *Habitual Perspective,* dan *Perception Perspective.*

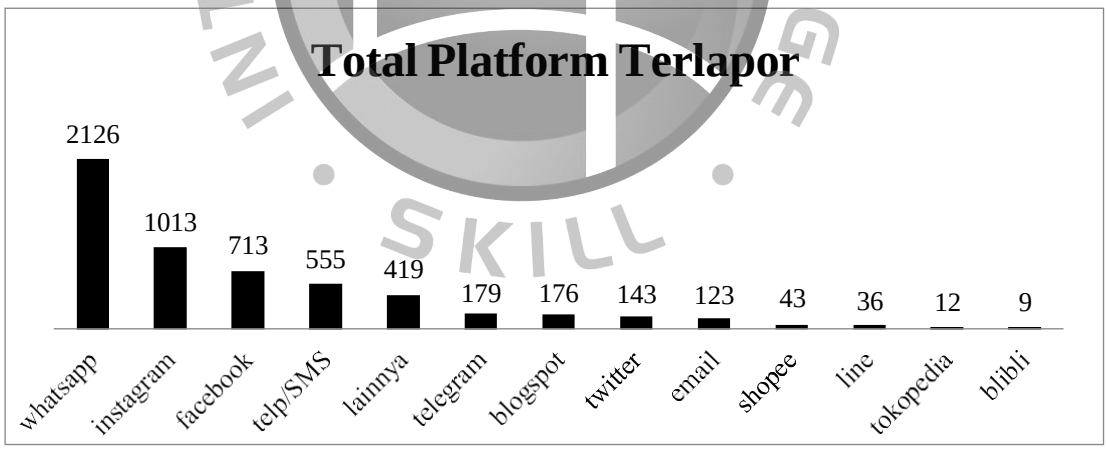
Manusia adalah makhluk yang kompleks dan kerentanannya mungkin tidak dapat dijelaskan dengan satu faktor perlu beberapa faktor yang dapat menjelaskan pengaruh kerentanan yang terjadi, pada aspek *Habitual Perspective*, dan *Perception Perspective* dapat melihat kemahiran manusai dalam mendeteksi rekayasa sosial.

Rekayasa sosial merupakan alat penyerang yang paling kuat yang dapat digunakan untuk mengakses pengetahuan dan memanipulasi seseorang untuk memberikan informasi kepada pelaku. Ini lebih unggul daripada kebanyakan bentuk peretasan lainnya karena dapat menembus sistem yang paling aman sekalipun, karena

pengguna itu sendiri adalah bagian yang paling rentan dari sistem (Krombholz et al.,2015). Lalu rekayasa sosial juga menyebabkan kerugikan operasi pemasaran dan kinerja pasar saham perusahaan, maka dari itu perusahaan bisnis dan

pemangku kepentingan mereka ingin menghentikan kejahatan dunia maya.

Aplikasi pesan instan, seperti Facebook Messenger dan WhatsApp, telah menjadi media penting untuk interaksi pribadi dengan teman dan keluarga. Dengan popularitas maka meningkat pula minat untuk menggunakan saluran-saluran ini untuk tujuan komersial. Facebook meluncurkan WhatsApp Bisnis. Pada Januari 2020, merek dapat memulai percakapan obrolan pribadi dengan konsumen langsung melalui *chat* via WhatsApp, seperti yang dilakukan konsumen ini dengan teman atau keluarga. Percakapan obrolan ini dapat terjadi dengan karyawan atau dengan chatbot (yaitu, agen percakapan yang diprogram untuk berkomunikasi dengan orang-orang melalui bahasa alami, dan dapat menjawab secara otomatis (Zarouali et al., 2021). Dan banyaknya individu maupun kelompok menggunakan aplikasi sosial media *WhatsApp*, maka disitulah celah bagi para pencuri data untuk melakukan aksinya agar mendapatkan data-data rahasia perusahaan maupun data pribadi. Dari laman https://www.patrolisiber.id/home pada bulan Januari 2021 sampai bulan Mei 2021 terdapat total aduan 4.453 aduan dan total kerugian 2,77 Triliun rupiah, berikut data penyerangan siber per platform yang terjadi di Indonesia



Gambar 1.1 Total aduan masyarakat kejahatan siber per platform media sosial
Sumber: https://www.patrolisiber.id/statistic, Data diolah penulis (2021)

Dikutip dari laman tekno.kompas.com sebelum adanya kemajuan teknologi yang begitu pesat, rekayasa sosial juga sudah dilakukan. Kebanyakan penipuan dilakukan dengan cara memanipulasi sisi psikologis dari korbannya, sehingga korban akan dengan mudah jatuh kedalam jebakan sang penipu.

Dengan begitu ada baiknya bagi kita untuk memperluas pengetahuan kita mengenai rekayasa sosial yang sering terjadi di masyarakat. “Saat ini, setiap hari ada sekitar 35.000 malware yang disebar oleh pelaku kejaharan siber. Sekitar 92% malware yang tersebar melalui surat elektronik. OJK berniat untuk meningkatkan kemampuan literasi konsumen serta meningkatkan kesadaran akan bahaya atas adanya kejahatan siber. OJK juga menyebarluaskan panduan keamanan bertransaksi digital”berikut berita yang dilansir oleh (Fernandez 2020) dalam situs ekonomi.bisnis.com, maka dari ituliterasi mengenai kejahatan siber dibutuhkan oleh masyarakat Indonesia.

1.2 Ruang Lingkup Masalah

Adapun ruang lingkup dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini merupakan modifikasi dari penelitian sebelumnya yang ditelitioleh (Albladi & Weir, 2020) “*Predicting individuals’ vulnerability to socialengineering in social network*”
2. Penelitian ini akan melakukan metodologi melalui survei kuantitatif dengan unit analisa pelajar dan atau karyawan produktif usia muda. Model akan
   dipecah menjadi tiga perspective yaitu *Habitual Perspective,* dan *PerceptionPerspective*
3. Variable yang digunakan dalam penelitian ini adalah *Habitual Perspective, Perception Perspective,* dan *Susceptibility*

1.3 Identifikasi Masalah

Berdasarkan pengamatan latar belakang diatas bahwa peristiwa ini merupakan peristiwa *Susceptibility* pada aplikasi sosial media *WhatsApp.* Dengan adanya peristiwa ini akan menunjukan apakah terdapat reaksi suatu individu yang tercermin dari *Habitual perspective,* dan *Perception Perspective* sehingga dapat diketahui seberapa pentingnya literasi mengenai *Social Engineering* untuk dipelajarilebih lanjut.

1.4 Rumusan Masalah

Berdasarkan penelitian terdahulu dengan *Scenario-based experiment* yang

telah dilakukan sebelumnya, maka penulis menentukan penelitian bagaimana pengaruh *Habitual perspective,* dan *Perception Perspective* terhadap *Susceptibility* sosial media *WhatsApp* :

1. Apakah terdapat perbedaan akibat efek *Habitual Perspective* terhadap *Susceptibility Scenario* pada aplikasi *WhatsApp*
2. Apakah terdapat perbedaan akibat efek *Perception Perspective* terhadap *Susceptibility Scenario* pada aplikasi *WhatsApp*

1.5 Batasan Masalah

Berdasarkan rumusan masalah diatas dapat disimpulkan bahwa peristiwa ini adalah peristiwa *Social Engineering* yang berguna untuk menunjukkan apakah terdapat reaksi individu yang tercermin dari *Habitual perspective,* dan *Perception*

Perspective. Penelitian ini dapat melihat pengaruh individu terhadap *Susceptibility* pada aplikasi *WhatsApp*

1.6 Tujuan Penelitian

1. Mengetahui dan menganalisis apakah terdapat perbedaan perilaku individu yang tercermin dari *Habitual perspective* pada sosial media *WhatsApp*.
2. Mengetahui dan menganalisis apakah terdapat perbedaan perilaku individu yang tercermin dari *Perception Perspective* pada sosial media *WhatsApp*.
3. Mengetahui dan menganalisis apakah terdapat perubahan perilaku individu yang tercermin dari *Habitual Perspective* dan *Perception Perspective* terhadap Kerentanan Sosial pada sosial media *WhatsApp*.

1.7 Manfaat Penelitian

1. Bagi Mahasiswa, penelitian ini diharapkan dapat menjadi acuan dan gambaran dalam berhati-hati untuk menggunakan sosial media.
2. Bagi individu atau organisasi, dengan adanya penelitian ini diharapkan dapatmemberikan gambaran dalam menggunakan sosial media.
3. Bagi para akademisi, penelitian ini diharapkan dapat membuka wawasan

baru mengenai kerentanan *Social Engineering* pada aplikasi sosial media dan dapat dikembangkan lagi pada sosial media lainnya untuk penelitian lanjutan.

1.8 Sistematika Penulisan

Sistematika penulisan ditujukan untuk memberikan gambaran secara keseluruhan tentang isi dari penelitian ini. Oleh karena itu, sistematika dalam penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini merupakan pendahuluan yang memberikan gambaran latar belakang penelitian ini mengenai kerentanan *Social Engineering* pada sosial media beserta data pelaporan penipuan dalam sosial media. Kemudian, terdapat juga rumusan masalah, batasan penelitian, tujuan penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini merupakan kelanjutan dari bagian pendahuluan yang di dalamnya terdapat landasan teori yang menjelaskan Grand Theory, variabel – variabel penelitian, penelitian terdahulu, kerangka pemikiran dan pengembangan hipotesis.

BAB III METODOLOGI PENELITIAN

Bab ini akan menjelaskan desain penelitian. Metode penelitian, metode pengambilan sampel hingga teknik pengolahan analisis data dan teknik pengujian hipotesis.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini akan memaparkan hasil penelitian menggunakan metodologi yang diusulkan melalui survei kuantitatif dengan unit analisa pelajar dan atau karyawan produktif usia muda. Data akan dikumpulkan dengan total target responden 110 dan kemudian dianalisa dengan bantuan statistik tool SmartPLS

dengan metode SEM

BAB V PENUTUP

Bab ini akan berisikan kesimpulan dan hasil penelitian yang diperoleh dari pembahasan sebelumnya. Dalam bab ini juga sebutkan kesimpulan, saran dan keterbatsan penelitian untuk peneliti selanjutnya.